Cybercriminology Foundations

CYBERCRIME

THE THEFT BEHIND IT

Brianna Martin, Marshall Brown, Sage Hensley, and Kendal Taylor

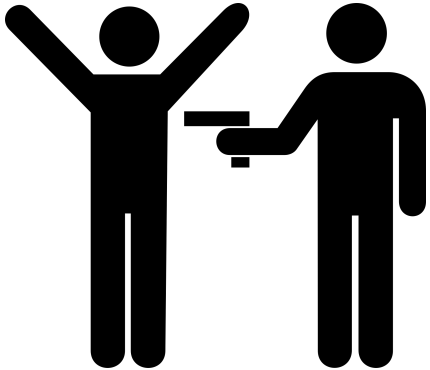
Introduction

Cyber criminology is one of the most important areas in the field of Cybersecurity. Learning it helps us understand, prevent, and respond to the ongoing threats that are happening everyday in our world. It covers four key areas which are Cyberviolence, Cybertrespass, Cyberpornography, and Cyber fraud. Each of these involves different types of online crimes. Cyberviolence is about crimes against a person. Cybertrespass involves a crime against digital property. Cyberpornography is crimes against society or morality. Finally, Cyber Fraud are crimes committed with the intent to gain access to sensitive information of an individual or business. However, Cyber Fraud is becoming one of the worst online crimes in the 21st century. Recently, there's been a huge Social Security Number leak across the U.S. leading to serious issues like identity theft and fraud. This project will dive into the 4 categories of Cyber Criminology, and how these SSNs are being stolen, why it's happening, and possible ways to identify if your data has been stolen or not.

Comparing/Contrasting the Different Types of Cybercrime

To compare and contrast, we must first define each of the categories as they are described in the textbook.

- **Cyberviolence** involves crimes against a person.
- **Cybertrespass** is crimes against property.
- **Cyberfraud** includes white-collar crimes and economic and workplace crimes.
- **Cyberpornography** is crimes against society or morality.



Comparisons in the Categories of Cybercrime

01

All cyber crimes involve violation/theft of both privacy and security.

- **Cybertrespass** and **cyberpornography** inolve sharing and/or stealing private material from their victims.
- **Cyber Violence** and **cyber fraud** both involve the exploitation of private information that can be used for stalking, blackmailing, or doxxing.

02

All cyber crimes cause psychological harm to their victims.

- **Cybertrespass** can cause victims to feel paranoid and violated, knowing their personal information is in someone else's possession.
- **Cyberpornography** can cause shame, embarrassment, and can sometimes even lead to suicide.
- **Cyber Fraud** can instill fear, stress, and depression as a result of financial loss.

03

Most cyber crimes are motivated by some sort of financial gain.

- **Cyber Trespassers** often sell the data they steal, or demand ransom for it.
- **Cyberpornography** is often sold, or perpetrators demand money using stolen images as blackmail.
- **Cyber Fraud** is almost exclusively financially motivated.
- **Cyberviolence** can be used as blackmail for money.

Contrasts in the Categories of Cybercrime

Some of the contrasts in different types of cybercrime include their most common **threat actors** and the **methods** they use to execute.

Category:	*Cyberpornography*	*Cyberviolence*
Threat Actors Include:	Adult content producers, acquaintances of victim, pimps, customers, child pornography offenders.	Bullies, stalkers, trolls, flamers.
Methods of Execution:	Revenge porn, unauthorized leaking of explicit images, child pornography.	Threats, harassment, trolling, cyberstalking, posting false messages about a victim, and flaming.

Contrasts in the Categories of Cybercrime cont.

Category:	*Cyber Fraud*	*Cybertrespass*
Threat Actors Include:	Identity thieves, fraudsters, scammers, malware developers, social engineers.	Hackers, script kiddies, hacktivists, insider threats.
Methods of Execution:	Phishing, vishing, smishing, romance scams, selling of counterfeit goods, advance fee frauds.	Hacking, malware, viruses, worms, trojans, impersonation, database exploitation.